EXHIBIT A

From: Simoes, Chris [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=2B20BBDA220D42FC9FFD190C207A5EAC-SIMOES, CHR]
Sent: 11/22/2019 2:58:27 PM
To: Pohorelsky, Pavel [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=79d8dfa5e5ed4a749691f6c0226408e7-Pohorelsky,]
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Nice work Pavel, thanks for the follow through and closing this out with me.

-Chris

From: "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>
Date: Friday, November 22, 2019 at 7:11 AM
To: "Simoes, Chris" <chris.simoes@solarwinds.com>
Subject: FW: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Chris,

The security issue I was referring to you on Tuesday is pretty much closed now. The accounts has been disabled the same day, I talked to the intern who deleted whole project from GitHub. Now RM team is in verification process, if any files there has been altered. It is highly unlikely, but we want to double check anyway.

--poho

From: "Sejna, Tomas" <tomas.sejna@solarwinds.com>
Date: Friday, 22 November 2019 at 13:18
To: "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>, "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>, "Zila, Josef" <josef.zila@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Sounds like a plan, thanks Lee.

solarwinds
Tomas Sejna | Senior Security Engineer
Office: +420 511 120 674

From: "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>
Date: Friday, 22 November 2019 at 13:17
To: "Sejna, Tomas" <tomas.sejna@solarwinds.com>, "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>, "Zila, Josef" <josef.zila@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: RE: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

We have 5707 files to be compared. We will provide an update by End of November on our progress.

Thank you,

solarwinds
Lee Zimmerman | Software Release Manager
Office: 512.682.9300 | Mobile: 512.415.1034

From: Sejna, Tomas
Sent: Friday, November 22, 2019 1:04 PM
To: Pohorelsky, Pavel <Pavel.Pohorelsky@solarwinds.com>; Zila, Josef <josef.zila@solarwinds.com>; Zimmerman, Lee <Lee.Zimmerman@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Perfect, I'll provide communication back to the researcher. We will keep the incident open, till the checksums are compared.

solarwinds
Tomas Sejna | Senior Security Engineer
Office: +420 511 120 674

From: "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>
Date: Thursday, 21 November 2019 at 15:29
To: "Zila, Josef" <josef.zila@solarwinds.com>, "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>, "Sejna, Tomas" <tomas.sejna@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

I updated the CP with this status:

- The login has been disabled during Tuesday 19th, nobody can access Akamai using these credentials anymore
- The mentioned GIthub has been deleted during Thursday 21st so it is not visible anymore
- Per information from release management, they are working on double checking that no files on Akamai has been modified. Because we are using signed executables, it is very unlikely but we are double cheking it anyway. Once this process is finished, this security incident can be closed.

External party can be announced, that we have eradicated the problem.

--poho

From: "Zila, Josef" <josef.zila@solarwinds.com>
Date: Tuesday, 19 November 2019 at 23:26
To: "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>, "Sejna, Tomas" <tomas.sejna@solarwinds.com>, "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: RE: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

According to Akamai support, only 3 IPs accessed the storage group in last 6 hours:

IP Address Lookup

IP: 67.79.13.42 Lookup

IP Address	67.79.13.42
ASN	20251
City	Austin
State/Region	Texas
Country Code	United States
Postal Code	78764
ISP	SolarWinds 3rd Try
Time Zone	-05:00

IP Address	67.79.13.42
ASN	20251
City	Austin
State/Region	Texas
Country Code	US
Postal Code	78735
ISP	SolarWinds, Inc.
Time Zone	America/Chicago

The first one is me and others checking the access from office

IP: 62.209.223.226 Lookup

IP Address	62.209.223.226
ASN	5588
City	Plzen
State/Region	Plzensky kraj
Country Code	Czech Republic
Postal Code	301 00
ISP	T-Mobile Czech Republic a.s.
Time Zone	+01:00

IP2Location.com Results

IP Address	62.209.223.226
ASN	5588
City	Vracov
State/Region	South Moravian
Country Code	CZ
Postal Code	696 42
ISP	T-Mobile Czech Republic a.s.
Time Zone	Europe/Prague

ipdata.co Results

The second one is me checking the access over my phone

IP Address Lookup

IP: 91.224.49.89 Lookup

IP Address	91.224.49.89
ASN	24641
City	Brno
State/Region	Jihomoravsky kraj
Country Code	Czech Republic
Postal Code	614 00
ISP	DPvt spol. s.r.o.
Time Zone	+01:00

IP2Location.com Results

IP Address	91.224.49.89
ASN	24641
City	Brno
State/Region	South Moravian
Country Code	CZ
Postal Code	623 00
ISP	FASTER CZ spol. s r.o.
Time Zone	Europe/Prague

ipdata.co Results

The third one is me checking from home.

So there was no one unauthorized accessing our Akamai storage group during last 6 hours. This does not necessarily mean that the compromised login information was not abused in the past, but at least we can be sure that no one was abusing it when we were trying to resolve the issue with Akamai.

From: Zimmerman, Lee
Sent: Tuesday, November 19, 2019 10:40 PM
To: Sejna, Tomas <tomas.sejna@solarwinds.com>; Zila, Josef <josef.zila@solarwinds.com>; Pohorelsky, Pavel <Pavel.Pohorelsky@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>; Zimmerman, Lee <Lee.Zimmerman@solarwinds.com>
Subject: RE: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

I just tried using the Credentials and got an error, so I believe it is no longer accessible via the solarwindsnet account. 10:38 PM Brno Time.

Thank you,

solarwinds
Lee Zimmerman | Software Release Manager
Office: 512.682.9300 | Mobile: 512.415.1034

From: Sejna, Tomas
Sent: Tuesday, November 19, 2019 3:16 PM
To: Zila, Josef <josef.zila@solarwinds.com>; Zimmerman, Lee <Lee.Zimmerman@solarwinds.com>; Pohorelsky, Pavel <Pavel.Pohorelsky@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Apologies, should be good from now on.

solarwinds
Tomas Sejna | Senior Security Engineer
Office: +420 511 120 674

From: "Zila, Josef" <josef.zila@solarwinds.com>
Date: Tuesday, 19 November 2019 at 15:14
To: "Sejna, Tomas" <tomas.sejna@solarwinds.com>, "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>, "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: RE: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Hi Tomas,

both me and Lee don't have permission to access that page:

You don't have permission to view this page

This is because it's inheriting restrictions from a parent page.
A space admin or the person who shared this page may be able to give you access.

From: Sejna, Tomas
Sent: Tuesday, November 19, 2019 3:09 PM
To: Zimmerman, Lee <Lee.Zimmerman@solarwinds.com>; Pohorelsky, Pavel <Pavel.Pohorelsky@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>; Zila, Josef <josef.zila@solarwinds.com>
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Incident page created, link for a quick navigation below.

https://cp.solarwinds.com/display/OP/2019-462%3A+GitHub+Public+Repo+FTR+Credentials+Leakage

I'd like you ask for routing all relevant updates to mentioned page so we can avoid email snowballing effect. Could an attacker affect integrity of stored installers with this attack vector? Great response with removing leaked credentials, let's follow with JIRA case for a tracking purpose. If you have any questions or need anything to help with, just give me a holler.

Thanks

solarwinds
Tomas Sejna | Senior Security Engineer
Office: +420 511 120 674

From: "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>
Date: Tuesday, 19 November 2019 at 14:57
To: "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>, "Sejna, Tomas" <tomas.sejna@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>, "Zila, Josef" <josef.zila@solarwinds.com>, "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>
Subject: RE: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

I will set up the new Upload account and work with NPM team to get it into the MIB tool. Update: the credentials have been removed from Akamai for solarwindsnet but we are waiting on the propagation to complete for the access to be removed.

Propagation Information

Following changes to this upload account are propagating:

- FTP Password addition *(2019-11-19T13:29:06Z by lee.zimmerman@solarwinds.com)*
- FTP Password deletion *(2019-11-19T12:59:04Z by josef.zila@solarwinds.com)*

Thank you,

solarwinds
Lee Zimmerman | Software Release Manager
Office: 512.682.9300 | Mobile: 512.415.1034

From: Pohorelsky, Pavel
Sent: Tuesday, November 19, 2019 2:50 PM
To: Zimmerman, Lee <Lee.Zimmerman@solarwinds.com>; Sejna, Tomas <tomas.sejna@solarwinds.com>

Cc: SolarWinds InfoSec <infosec@solarwinds.com>; Zila, Josef <josef.zila@solarwinds.com>
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

NPM team responsible for MIB uploads are aware about this change. It might make sense moving forward to use special account only for MIB uploads with account rights limited only to this specific action.

--poho

From: "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>
Date: Tuesday, 19 November 2019 at 14:12
To: "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>, "Sejna, Tomas" <tomas.sejna@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>, "Zimmerman, Lee" <Lee.Zimmerman@solarwinds.com>, "Zila, Josef" <josef.zila@solarwinds.com>
Subject: RE: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

This was a previous password for the main Akamai Upload Account. It was still in an active state. It is now removed from this upload account as of 2:00 PM Brno Time. Impact to this action will be the need to provide new credentials for the MIB update Tool. We may consider the UserName compromise and no longer use this account going forward.

Thank you,

solarwinds
Lee Zimmerman | Software Release Manager
Office: 512.682.9300 | Mobile: 512.415.1034

From: Pohorelsky, Pavel
Sent: Tuesday, November 19, 2019 2:05 PM
To: Sejna, Tomas <tomas.sejna@solarwinds.com>; Zimmerman, Lee <Lee.Zimmerman@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: Re: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Hi,

I am confirming that the mentioned credentials are valid credentials for installer uploads to akamai. I confirmed this with @Zimmerman, Lee who is changing the password right now. He is on CC of this conversation so he can provide more details if needed.

What are the next steps?

--poho

From: "Sejna, Tomas" <tomas.sejna@solarwinds.com>
Date: Tuesday, 19 November 2019 at 11:39
To: "Pohorelsky, Pavel" <Pavel.Pohorelsky@solarwinds.com>
Cc: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: FW: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

Hi Pavel,

We have received an inquiry about hard-coded credentials, which are publicly available and allows attacker to upload files to our FTP download server. It seems like a part of university thesis by one of our former interns Adam Kozusnik, who worked at NPM. With that being said, I'd like to ask you for a validation, so we can move communicate back to the researcher.

Thanks

solarwinds
Tomas Sejna | Senior Security Engineer
Office: +420 511 120 674

From: SolarWinds PSIRT <PSIRT@solarwinds.com>
Date: Tuesday, 19 November 2019 at 10:10
To: SolarWinds InfoSec <infosec@solarwinds.com>
Subject: A new EXTERNAL inquiry has been submitted by: Vinoth Kumar

A new external notification or inquiry has been submitted and needs to be reviewed to determine if it should be classified as an incident.

Summary:

1. Type of submission: Security Vulnerability

2. Submitted by: Vinoth Kumar with an email address of: vinothsparrow@live.com

3. Company:

4. Date Submitted: Tuesday, November 19, 2019 3:09 AM

5. Description Provided: Hi Team, I have found a public Github repo which is leaking ftp credential belongs to SolarWinds. Repo URL: https://github.com/xkozus00/mib-importer/blob/master/Src/Lib/PurgeApp/PurgeApp.exe.config Downloads Url: http://downloads.solarwinds.com FTP Url: ftp://solarwinds.upload.akamai.com Username: solarwindsnet Password: solarwinds123 POC: http://downloads.solarwinds.com/test.txt I was able to upload a test POC. Via this any hacker could upload malicious exe and update it with release SolarWinds product.

Details of what was submitted can be reviewed in the SharePoint document library here: PSIRT Reported Vulnerabilities

THIS IS AN AUTO-GENERATED MESSAGE from Microsoft Flow